Applicants respectfully reassert the relevant remarks made with respect to the Lewis reference and the Ellison article in their previous response and further note that the cited references are silent as to providing selectable expiry periods for private signing keys. Applicants also note that the references teach away from Applicants' claimed invention and teach away from each other. For example, the Ellison article teaches away from identity based certificates such as those that include a user's name and instead teaches using a generalized certificate wherein a user generates the certificate and the certificate does not have a user name therein. (See Ellison article, p. 2, Section entitled "Generalized Certificate", 1st paragraph; p. 3, Section entitled "Certificate Structure". In contrast, Applicants claim a multi-client unit that provides selectable expiry data associated with a private signing key (not described by the references) and the public verification key. Also, Ellison, as noted in previous responses, is not believed to be enabling and also Ellison appears to describe that client units generate their own certificates which is an opposite approach to Applicant's claimed invention. Accordingly, the claim is believed to be allowable.

As to the other pending claims, Applicants again respectfully request factual support as to why one of ordinary skill in the art would look to the Ellison reference, which teaches against the use of certification authorities and conventional certificates and also teaches the elimination of certificate revocation lists, and is silent as to updating digital signature key pairs for a plurality of clients, for teachings related to a key replacement and to a system described in Lewis that requires the use of a key replacement message that contains the replacement public key and contains the mask of the next replacement key. Ellison is not at all directed to key replacement techniques. Applicants again note that the law requires that a combination of references must be made with no knowledge of the claimed invention and hence particular findings and selective

teachings cannot be combined with knowledge of the Applicants' claimed invention. Applicants respectfully submit that it appears that impermissible hindsight may have been used in combining these references since they are dealing with different problems, describe unrelated solutions and alone or in combination fail to disclose the claimed invention.

Also, the Ellison reference, as understood by one of ordinary skill in the art, has its focus directed to avoiding the use of certification authorities. See for example p. 4 where the Ellison article states "This means that most cases, there is no need for a formal certification authority (whose existence is devoted to assuring the binding between a physical person and a public key)." The article goes on to state that generalized certificates should be used instead and that CRLs should not be used and are ineffective.

Applicants' invention is related to when to roll over keys which should occur prior to the invalidity of a certificate to avoid for example, the ability of a user to access information or digitally sign information. The problem faced by Ellison is not at all related to rolling over keys or updating key pairs and teaches away from a multi-client manager unit as claimed, since Ellison, among other things, teaches to avoid using certification authorities or other multi-client manager operations.

Applicants respectfully submit that the claims are in condition for allowance and a Notice of Allowance is respectfully solicited. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a conference would expedite the prosecution of the instant application.

Dated: January 8, 2003

Respectfully submitted,

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz
222 N. LaSalle Street, Suite 2600
Chicago, IL 60601
PH: (312) 609-7599
FAX: (312) 609-5005